AIOps Certified Professional Certification for DevOps and SRE Teams

Introduction

IT operations have changed significantly. Applications now run across cloud platforms, containers, Kubernetes clusters, distributed services, and hybrid infrastructure. As these environments grow, engineering teams receive more alerts, logs, metrics, and incidents than they can efficiently handle through manual monitoring alone.This is where **AIOps** becomes useful.AIOps applies artificial intelligence, machine learning, analytics, observability, and automation to IT operations. Its purpose is to help teams understand system behaviour, identify unusual activity, reduce unnecessary alerts, speed up troubleshooting, and automate repetitive operational tasks.The **AiOps Certified Professional (AIOCP)** certification from DevOpsSchool is designed for professionals who want to develop practical knowledge of AIOps and its connection with DevOps, cloud operations, monitoring, machine learning, and incident automation.

AIOCP Certification Snapshot

Area	Details
Certification	AiOps Certified Professional (AIOCP)
Provider	DevOpsSchool
Track	AIOps, Observability, Automation, IT Operations
Level	Intermediate
Suitable for	Engineers, SREs, DevOps professionals, cloud teams, managers
Useful background	Linux, cloud, scripting, containers and monitoring
Main skills	Monitoring, anomaly detection, event analysis, ML workflows, automation
Suggested sequence	Foundations → Monitoring → Analytics → Automation

Understanding the AIOCP Certification

What it is

AIOCP is a professional learning and certification path focused on intelligent IT operations.

Instead of concentrating only on monitoring tools, it introduces learners to the complete operational flow: collecting data, identifying abnormal behaviour, analyzing incidents, using machine learning, and automating responses.

Who Can Benefit From AIOCP?

The certification can be relevant for professionals working in both development and operations.

It may be suitable for:

- Software Engineers
- DevOps Engineers
- Site Reliability Engineers
- Cloud Engineers
- Platform Engineers
- Infrastructure Engineers
- System Administrators
- Operations Teams
- Technical Leads
- Engineering Managers
- MLOps Engineers
- Professionals moving into AIOps roles

For software engineers, AIOps knowledge can improve understanding of how applications behave after deployment.

For operations teams, it can help strengthen monitoring, incident management, and automation practices.

For managers, it provides a better understanding of how intelligent operations can improve reliability and reduce manual operational work.

Knowledge That Helps Before Starting

A learner does not need to be an expert in every technology, but some basic technical knowledge can make the learning process easier.

Useful areas include:

- Linux commands and system basics
- Basic Python or Bash scripting
- Cloud computing fundamentals
- Docker and container concepts
- Kubernetes basics
- Monitoring and alerting concepts
- Logs, metrics, traces, and events
- Basic DevOps understanding

These skills create the foundation required to understand more advanced AIOps concepts.

Important Skills Covered in AIOps Learning

AIOps combines several technical disciplines.

Learners should expect to build knowledge in areas such as:

- Infrastructure and application monitoring
- Log collection and analysis
- Metrics-based monitoring
- Distributed tracing
- Observability practices
- Anomaly detection
- Event correlation
- Alert prioritization
- Operational analytics
- Machine learning workflows
- Incident management
- Automated runbooks
- Infrastructure automation
- Self-healing systems
- Cloud and Kubernetes monitoring

The real value comes from understanding how these areas work together rather than learning them separately.

How AIOps Works in a Real Environment

A simple AIOps workflow can look like this:

Collect data → Detect unusual activity → Analyze related events → Identify possible cause → Trigger action → Verify recovery

For example, imagine an application suddenly becomes slow.

A traditional monitoring system may only report high CPU usage.

An AIOps-based approach may also examine:

- Recent application deployments
- Database performance
- Kubernetes events
- Service latency
- Error logs
- Infrastructure changes
- Previous incidents

Using this information, the system can help operations teams identify the most likely cause and recommend or trigger an appropriate response.

Practical Projects to Build After Learning AIOps

AIOps becomes easier to understand when learners build real projects.

Useful project ideas include:

- Centralized log monitoring setup
- Kubernetes monitoring dashboard
- Prometheus and Grafana observability project
- OpenTelemetry implementation
- Application tracing setup
- Basic anomaly detection system
- Alert grouping and correlation workflow
- Incident notification automation
- Automated remediation runbook
- Kubernetes auto-recovery workflow
- Infrastructure monitoring project
- ML-based operations analytics project

These projects help demonstrate practical knowledge beyond certification theory.

A Simple Preparation Approach

7–14 Day Plan

This approach is suitable for professionals already familiar with DevOps and cloud technologies.

Focus mainly on:

- AIOps concepts
- Observability
- Kubernetes monitoring
- Prometheus and Grafana
- Anomaly detection
- Incident management
- Automation workflows
- Scenario-based practice

Spend more time on practical use cases than basic technical fundamentals.

30 Day Plan

A 30-day plan gives learners more time to combine theory and practice.

Week 1: Linux, scripting, cloud and containers

Week 2: Kubernetes, logs, metrics, traces and observability

Week 3: AIOps concepts, anomaly detection and machine learning basics

Week 4: Incident automation, remediation and practical projects

This approach works well for working professionals who can study consistently each day.

60 Day Plan

A 60-day plan is better for learners who need stronger fundamentals.

Start with Linux, cloud, Python, Docker, and Kubernetes.

Then move into monitoring and observability.

After that, study anomaly detection, machine learning workflows, incident correlation, and automation.

Use the final part of the preparation period to build projects and practice operational scenarios.

Mistakes to Avoid While Learning AIOps

Many learners focus too heavily on tools.

This can create gaps in understanding.

Common mistakes include:

- Learning commands without understanding operational problems
- Assuming AIOps means only artificial intelligence
- Ignoring observability fundamentals
- Using poor-quality monitoring data
- Creating excessive alerts
- Ignoring false-positive alerts
- Automating recovery without proper checks
- Avoiding hands-on practice
- Studying only to pass the certification

A good AIOps professional should understand both the technology and the operational problem being solved.

Choose Your AIOps Learning Path

AIOps can connect with several technology career paths.

DevOps Path

Recommended sequence:

DevOps → Cloud → Docker → Kubernetes → Observability → Automation → AIOps

This path is suitable for professionals responsible for software delivery and infrastructure automation.

DevSecOps Path

Recommended sequence:

DevOps → Security Fundamentals → Cloud Security → Container Security → Security Monitoring → Automated Response → AIOps

This path can help professionals combine operational intelligence with security monitoring.

SRE Path

Recommended sequence:

Linux → Cloud → Kubernetes → Observability → Reliability Engineering → Incident Management → AIOps

SRE professionals can use AIOps to improve incident detection, alert quality, and automated recovery.

AIOps/MLOps Path

Recommended sequence:

Python → Data Fundamentals → Machine Learning → MLflow → Model Monitoring → Observability → AIOps

This is suitable for professionals interested in combining operations with machine learning.

DataOps Path

Recommended sequence:

Data Engineering → Data Pipelines → Data Quality → Data Monitoring → Analytics → AIOps

AIOps depends heavily on reliable operational data, making DataOps knowledge valuable.

FinOps Path

Recommended sequence:

Cloud → Usage Monitoring → Cost Management → Cost Anomaly Detection → Automation → AIOps

This path is useful for professionals focused on cloud efficiency and cost optimization.

What Certification Can Come After AIOCP?

The right next certification depends on career goals.Professionals interested in reliability can move toward SRE or observability-focused certifications.DevOps professionals may continue with cloud, Kubernetes, infrastructure automation, or platform engineering.Those interested in artificial intelligence can explore MLOps or machine learning certifications.Security professionals may continue with DevSecOps, while professionals focused on data or cost management may choose DataOps or FinOps.The goal should be to build deeper expertise rather than collect unrelated certifications.

Training and Certification Support Platforms

Professionals looking for additional learning support can explore different training and technical education platforms.

Some commonly considered names in this ecosystem include:

- DevOpsSchool
- Cotocus
- Scmgalaxy
- BestDevOps
- devsecopsschool
- sreschool
- aiopsschool
- dataopsschool
- finopsschool

Before choosing a provider, compare the syllabus, practical labs, project work, instructor support, learning format, and relevance to your target role.

Conclusion

The **AiOps Certified Professional (AIOCP)** certification can help professionals understand how intelligent automation is changing IT operations. It brings together monitoring, observability, machine learning, incident management, cloud technologies, and automation into one practical learning path. The strongest way to prepare is to combine technical fundamentals with hands-on projects and real operational scenarios. Professionals working in DevOps, SRE, cloud, MLOps, DataOps, DevSecOps, or FinOps can use AIOps knowledge to improve how modern systems are monitored, analyzed, and managed.